CLAIMS

What is claimed is:

1. A network analyzer for use in a computer network having wireless components providing encrypted data transmission and having at least two wireless access points with different encryption keysets, said network analyzer comprising:

at least one wireless card adapted to receive encrypted data on one or more channels that said at least two wireless access points are using; and

a single keyset profile stored in a data store, said single keyset profile having a plurality of encryption keysets, each encryption keyset being used to decrypt encrypted data received from a different access point of said at least two wireless access points, said keyset profile being used to decrypt all of said encrypted data without having to manually enter a key or keyset information into said analyzer.

2. The network analyzer of claim 1, wherein said encrypted data is stored in non-volatile memory before said data is decrypted.

3. The network analyzer of claim 1, wherein each access point of said at least two access points utilizes a unique keyset, wherein said profile contains each unique keyset.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

4. The network analyzer of claim 1, wherein said single keyset profile comprises a plurality of encryption keysets with each encryption keyset comprising at least two keys.

5. The network analyzer of claim 1, wherein each of said access points operates on a different AP channel.

6. The network analyzer of claim 5, wherein said at least one wireless card receives encrypted data from each of said access point channels for a period of time.

7. The network analyzer of claim 1, wherein said at least one wireless card alternately receives encrypted data from each of said access points until said at least one wireless card receives a defined quantity of encrypted data from each of said access points.

8. The network analyzer of claim 1, wherein said data store is either volatile or non-volatile memory.

9. The network analyzer of claim 8, wherein said encrypted data is stored in a data buffer before being stored in said data store.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

10. The network analyzer of claim 1, further comprises an analyzer, said analyzer decrypting said encrypted data received by said at least one wireless card using each of said plurality of encryption keysets in sequence until all of said encrypted data has been decrypted.

11. The network analyzer of claim 1, wherein each of said keysets uses at least 64 bit encryption.

12. The network analyzer of claim 1, wherein each of said keysets uses at least 128 bit encryption.

13. The network analyzer of claim 1, wherein said profile is stored internally in the network analyzer.

14. The network analyzer of claim 13, wherein said profile is encrypted.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

15. In a computer network having wireless components providing encrypted data transmission and receipt and comprising at least two wireless access points, said network having a different encryption keyset for each of said at least two access points, said computer network further comprising at least one computer being connected to said network by a wireless network card and having an analyzer module, a method for decrypting data captured by said wireless network card from at least one of said at least two access points, said method comprising:

a step for establishing a keyset profile accessible by the analyzer module, said keyset profile having all keysets being used by any of said at least two access points;

a step for receiving encrypted data from at least one of said at least two access points and saving said encrypted data to a data store; and

a step for decrypting said data in said data store using said keyset profile, wherein said data is decrypted without manually entering keys or keyset information.

16. The method of claim 15, wherein said step for saving said encrypted data further includes a step of saving said encrypted data to a data buffer before saving said data in said data store.

17. The method of claim 15, further comprising a step for analyzing said decrypted data to identify any encrypted data.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

18. The method of claim 15, further comprising a step for decrypting said encrypted data using a second keyset associated with said keyset profile.

19. The method of claim 18, further comprising a step for repeatedly analyzing and decrypting said encrypted data until said encrypted data is completely decrypted.

20. The method of claim 19, wherein said step for repeatedly analyzing and decrypting is performed without input from a user of said analyzer module.

21. The method of claim 15, further comprising a step for selecting said keyset profile for said at least two wireless access points.

22. The method of claim 15, further comprising a step for accessing said keyset profile at a location of said computer network remote from said analyzer module.

23. The method of claim 22, wherein said keyset profile is stored in an encrypted form and further comprising a step for decrypting said keyset profile and storing a decrypted version of said keyset profile local to said analyzer module.

24. The method of claim 15, further comprising a step for displaying said decrypted data through at least one user interface.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

25. An administrator system for use in a wireless computer network having a plurality of wireless access points that use different encryption keysets, the administrator system comprising:

a wireless card capable of receiving encrypted data from one or more channels of said plurality of wireless access points;

a data storage that stores the different encryption keysets in a single keyset profile; and

an analyzer electrically connected to said wireless card and said data storage, said network analyzer capable of decrypting said encrypted data captured from said one or more channels of said plurality of access points by said wireless network card, wherein said keyset profile is used to decrypt all of said captured encrypted data received from said plurality of wireless access points.

26. The administrator system of claim 25, wherein said captured encrypted data is stored in said data store.

27. The administrator system of claim 25, wherein said captured encrypted data is stored in a data buffer before said encrypted data is stored in said data store.

28. The administrator system of claim 27, wherein said captured encrypted data in said data buffer is written to said data store prior to being decrypted and wherein said analyzer decrypts said captured data by applying each unique keyset in sequence until all of said encrypted data has been decrypted.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

29. The administrator system of claim 28, wherein a user selects an order for said keysets to be used to decrypt said captured data.

30. The administrator system of claim 25, wherein each access point has a keyset that encrypts data to and from at least one user and said access points, said keyset profile containing said keyset to each of said plurality of access points.

31. The administrator system of claim 30, wherein each access point utilizes a unique keyset, and wherein said keyset profile contains each unique keyset.

32. The administrator system of claim 30, wherein said keyset for each access point utilizes at least two keys, and wherein said keyset profile contains each of said keysets.

33. The administrator system of claim 25, wherein each of said access points operates on a different AP channel.

34. The administrator system of claim 25, wherein said analyzer records said data on each of said access point channels for a period of time.

35. The administrator system of claim 34, wherein said analyzer rotates sequentially through all of said access point channels in a continuing loop.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

36. The administrator system of claim 35, wherein said period of time is approximately ten seconds.

37. The administrator system of claim 25, wherein each of said keysets uses at least 64 bit encryption.

38. The administrator system of claim 25, wherein each of said keysets uses at least 128 bit encryption.

39. The administrator system of claim 25, wherein said keyset profile is stored in said data store.

40. The administrator system of claim 25, wherein said data store is remote from said analyzer.

41. The administrator system of claim 40, wherein said keyset profile is stored in an encrypted form.

WORKMAN NYDEGGER
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111